Available online at www.sciencedirect.com

ScienceDirect

Journal of Number Theory 124 (2007) 42–56

JOURNAL OF Number Theory

www.elsevier.com/locate/jnt

Galois 2-extensions unramified outside 2

John Jossey

Department of Mathematics, University of Illinois, Urbana-Champaign, IL 61801, USA

Received 26 May 2006; revised 26 June 2006

Available online 24 October 2006

Communicated by Gebhard Böckle

Abstract

We classify quadratic, biquadratic and degree 4 cyclic 2-rational number fields. We also classify those quadratic number fields which are not 2-rational, but have a degree 2 extension, which is Galois over $\mathbb{Q}$ and is 2-rational. In this case we explicitly describe the Galois group of their maximal pro-2 extension unramified outside 2 and infinity using a result of Herfort–Ribes–Zalesskii on virtually free pro-p groups.

Keywords: Class number; Conductor; Dirichlet character; Genus field; Free pro-p product; Profinite group; Galois group; Virtually free pro-p group

1. Introduction and statement of results

Let K be a number field. Let S denote the set of prime divisors of p and the infinite primes of K, and $K_S(p)$ denote the maximal pro-p extension of K unramified outside S. Let G_S denote the Galois group $G(K_S(p)/K)$. The big problem is to determine G_S. There is a characterization for it to be a free pro-p group [9, Corollary 8.7.10]. Also K. Wingberg [14] has classified when it is Demuškin. A natural question to ask is for which number fields K is it a virtually free (Definition 8) pro-p group? In this paper we study the case when $p = 2$, and classify quadratic, biquadratic and degree 4 cyclic number fields whose G_S is free. We also classify those quadratic number fields for which G_S is not free, but has a degree 2 extension, which is Galois over $\mathbb{Q}$ and whose G_S is free. In this case we explicitly describe the Galois group of their maximal pro-2 extension unramified outside 2 and infinity using a result of Herfort–Ribes–Zalesskii (Theorem 10) on virtually free pro-p groups.

E-mail address: jossey@math.uiuc.edu.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2006.08.006

1.1. Notations

Let S_K be the set of prime divisors of 2 and the infinite primes in K. If K has a unique prime above 2, it will be denoted by P_K. Let $\mathcal{O}_K, U_K, h_K, Cl(K)$ denote the ring of integers, unit group, class number and the class group of K respectively. We will study the Galois extensions of K of degree a power of 2, unramified outside S_K, whose composite is the maximal pro-2 extension of K unramified outside S_K. The Galois group of the maximal 2-extensions of K unramified outside S_K will be denoted by G_{S_K}. Since the cyclotomic 2-extension of $\mathbb{Q}$ unramified outside 2 and infinity is infinite, G_{S_K} is an infinite pro-2 group.

Let L be an imaginary biquadratic extension of $\mathbb{Q}$ or an imaginary cyclic extension of $\mathbb{Q}$ of degree 4. Let g_2, e_2 and f_2 denote the number of prime factors, the ramification index and the inertial degree of 2 in L. Let $m > 1, n < 0$, be square free integers, $k = \frac{mn}{(m,n)^2}$. Let $L_+ = \mathbb{Q}(\sqrt{m})$ be the unique real quadratic subfield of L. Let $L_- = \mathbb{Q}(\sqrt{n})$, and let $F = \mathbb{Q}(\sqrt{k})$. Assume that there is a unique prime above 2 in L.

1.2. Definitions and statement of our results

The aim of this paper is to prove the following results.

Definition 1. A number field F is said to be p-rational if G_S is free.

Theorem 2. *Let K be a quadratic number field. Then K is 2-rational if and only if K is any imaginary quadratic subfield of $\mathbb{Q}(\zeta_{8p})$ where p is a prime $\equiv \pm 3 \bmod 8$. More precisely $K = \mathbb{Q}(\sqrt{n})$ is one of the following, $n = -1, -2, -p$ or $-2p$ where p is a prime $\equiv \pm 3 \bmod 8$. In each of the above cases $G_{S_{\mathbb{Q}(\sqrt{n})}} \cong \mathbb{Z}_2 \amalg \mathbb{Z}_2$ where $\amalg$ indicates the free pro-2 product.*

Theorem 3. *Let L be a cyclic extension of degree 4 over $\mathbb{Q}$ with L_+ as the unique quadratic subfield of L. Then L is 2-rational if and only if*:

(1) *The conductor of L has a unique prime factor and*
   (a) *L is the imaginary cyclic extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_p)$, where p is a prime $\equiv 5 \bmod 8$.*
   (b) *L is the imaginary cyclic extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_{2^4})$.*

(2) *The conductor of L has two prime factors and*
   (a) *L is an imaginary cyclic extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_{2^4 p})$ with $L_+ = \mathbb{Q}(\sqrt{2})$, where p is a prime $\equiv \pm 3 \bmod 8$ and $h_L \equiv 2 \bmod 4$.*
   (b) *L is an imaginary cyclic extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_{2^4 p})$ with $L_+ = \mathbb{Q}(\sqrt{p})$, where p is a prime $\equiv 5 \bmod 8$ and $h_L \equiv 2 \bmod 4$.*
   (c) *L is an imaginary cyclic extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_{2^4 p})$ with $L_+ = \mathbb{Q}(\sqrt{2p})$, where p is a prime $\equiv 5 \bmod 8$ and $2^2 \| h_L$*

In each of the above cases $G_{S_L} \cong \mathbb{Z}_2 \amalg \mathbb{Z}_2 \amalg \mathbb{Z}_2$ and $G_{S_{L_+}} \cong C_2 \amalg C_2 \amalg \mathbb{Z}_2$.

The following is our main result.

Theorem 4. *Let L be a biquadratic number field, then*:

(1) *L is 2-rational if and only if L is any imaginary biquadratic subfield of $\mathbb{Q}(\zeta_{8p})$, where p is a prime $\equiv \pm 3 \bmod 8$. More precisely, $L = \mathbb{Q}(\sqrt{n}, \sqrt{m})$, is one of the following*
   (a) *$n = -1$ and $m = 2$, p or $2p$ where p is a prime $\equiv \pm 3 \bmod 8$.*
   (b) *$n = -2$ and $m = p$ or $2p$ where p is a prime $\equiv \pm 3 \bmod 8$.*
   (c) *$n = -p$, where p is a prime $\equiv \pm 3 \bmod 8$ and $m = 2$.*

(2) *In each of the above cases $G_{S_{L_+}} \cong C_2 \amalg C_2 \amalg \mathbb{Z}_2$ and $G_{S_{L_-}}$ and G_{S_F} are free groups on 2 generators hence isomorphic to $\mathbb{Z}_2 \amalg \mathbb{Z}_2$ and $G_{S_L} \cong \mathbb{Z}_2 \amalg \mathbb{Z}_2 \amalg \mathbb{Z}_2$.*

The main idea in proving the above theorem, which is also the most recurring theme of this paper, is not to have too many finite ramified primes in L over $\mathbb{Q}$; in fact for L to be 2-rational, L cannot have more than 2 finite ramified primes.

Corollary 5. *Let K be a quadratic number field. Suppose K is not 2-rational. Then K has a degree 2 extension L, such that L is Galois over $\mathbb{Q}$ and is 2-rational if and only if K is any real quadratic subfield of $\mathbb{Q}(\zeta_{8p})$ where p is a prime $\equiv \pm 3 \bmod 8$ and in each of these cases $G_{S_K} \cong C_2 \amalg C_2 \amalg \mathbb{Z}_2$.*

Definition 6. A number field F is said to be minimal p-rational if F is p-rational and no proper subfield of F has this property.

Corollary 7. *The only minimal 2-rational degree 4 normal extensions of $\mathbb{Q}$ are the imaginary cyclic extensions of $\mathbb{Q}$ of Theorem 3.*

2. Preliminaries

2.1. Group theory

Let p be a rational prime and G a pro-p group, that is an inverse limit of finite p-groups.

Definition 8. [11, p. 121] A pro-p group G is virtually free if G has an open free subgroup.

Let $\{G_i \mid i = 1, \ldots, n\}$ be a collection of pro-p groups. Let $G^{abs} = G_1 * \cdots * G_n$ be the free product of $G_1, \ldots, G_n$ considered as abstract groups.

Definition 9. [10, Remark 9.1.3] The free pro-p product $G = G_1 \amalg \cdots \amalg G_n$ is the completion of G^{abs} with respect to the topology defined by the collection of all normal subgroups N of finite index in G^{abs} such that $N \cap G_i$ is open in G_i $(i = 1, \ldots, n)$ and G^{abs}/N is a finite p-group.

The following theorem is the group-theoretic fact which we use to deduce the structure of the G_{S_K}. It is also a generalization of a well-known result of Serre: "A torsion-free virtually free pro-p group is free."

Theorem 10. [15,4] *If G is a pro-p group having a free pro-p subgroup F of countable rank and index p then*

$$G \cong \left(\coprod_{x \in X} (C_p \times H_x) \right) \amalg H$$

is a free product, where C_p denotes the group of order p, H_x, H are free pro-p groups of F and X is the space of conjugacy classes of subgroups of order p in G.

In [4], the above theorem is stated without the restriction of F having a countable rank. In [15], P.A. Zalesskii corrects this error and gives an example of pro-2 group G having a free subgroup F of index 2 with uncountable rank, and G not having the above decomposition.

Definition 11. [12, p. 17] Let p be a prime number and G a profinite group. One calls the p-cohomological dimension of G, and uses the notation $cd_p(G)$, to denote the lower bound of the integers n which satisfy the following condition: For every discrete torsion G-module A, and for every $q > n$, the p-primary component of $H^q(G, A)$ is zero. One defines the cohomological dimension to be $cd(G) = \sup cd_p(G)$.

Let $Fr(G)$ denote the Frattini subgroup of G, i.e. the intersection of the kernels of the continuous homomorphisms $G \to \mathbb{F}_p$. Therefore $Fr(G) = \overline{G^p[G, G]}$ where $\overline{[G, G]}$ denotes the closure of the commutator subgroup of G. The groups $G/Fr(G)$ and $H^1(G, \mathbb{F}_p)$ are duals of each other. The minimum number of topological generators of G equals the minimum number of generators of $G/Fr(G)$, by Burnside's theorem. Therefore the minimum number of generators of G is $\dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p)$ [12, Section 4.2] or [6] or [7, Section 6.1], and the relation rank of G is $\dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p)$ [12, Section 4.3].

There is a mapping [6] or [7, Section 11.1]

$$\phi_S^* : H^2(G_S, \mathbb{F}_p) \longrightarrow \sum_{\wp \in S} H^2(G_\wp, \mathbb{F}_p)$$

where $G_\wp$ is Galois group of the maximal p-extension of $K_\wp$ and $K_\wp$ is the completion of K at $\wp$.

Let $\mathfrak{W}_S$ denote the kernel of ϕ_S^*.

Definition 12. ([6] or [7, Section 11.2]) Let $B_S = (V_S/K^{\times p})^*$, where

$$V_S = \left\{ \alpha \in K^\times \mid (\alpha) = \mathfrak{a}^p,\ \alpha \in K_\wp^p \text{ for } \wp \in S \right\}$$

where (α) is the principal fractional ideal generated by α, and $\mathfrak{a}$ is some fractional ideal in K and $*$ indicates the dual.

Theorem 13. ([6] or [7, Theorem 13.8]) *Suppose $\mu_p \subset K$. Then $\mathfrak{W}_S \cong B_S$ and there exists a map*

$$\sum_{\wp \in S} H^2(G_\wp, \mathbb{F}_p) \xrightarrow{\text{inv}} \mathbb{F}_p$$

such that the sequence

$$0 \longrightarrow B_S \longrightarrow H^2(G_S, \mathbb{F}_p) \longrightarrow \sum_{\wp \in S} H^2(G_\wp, \mathbb{F}_p) \longrightarrow \mathbb{F}_p \longrightarrow 0$$

is exact.

Remark 14. When $B_S = 0$, the map ϕ_S^* is injective. Hence all the global relations come from the local relations.

Theorem 15. ([9, Theorem 8.7.3] or [6] or [7, Theorems 11.8 and 11.5])

(1) $$\dim_{\mathbb{F}_p} H^1(G_S, \mathbb{F}_p) = 1 + \sum_{\wp \in S} \delta_\wp - \delta + \dim_{\mathbb{F}_p} B_S$$

where

$$\delta = \begin{cases} 1 & \text{if } \mu_p \subseteq K, \\ 0 & \text{if } \mu_p \nsubseteq K, \end{cases} \quad \text{and} \quad \delta_\wp = \begin{cases} 1 & \text{if } \mu_p \subseteq K_\wp, \\ 0 & \text{if } \mu_p \nsubseteq K_\wp. \end{cases}$$

Moreover if $\mu_p \subseteq K$, *then* $\dim_{\mathbb{F}_p} B_S = \dim_{\mathbb{F}_p} Cl_S/Cl_S^p$, *where*

$$Cl_S = Cl(K)/\langle S \rangle$$

where $\langle S \rangle$ *denotes the subgroup of* $Cl(K)$ *generated by the prime ideals in* S.

(2) $$\dim_{\mathbb{F}_p} H^2(G_S, \mathbb{F}_p) = \sum_{\wp \in S \setminus S_\mathbb{C}} \delta_\wp - \delta + \dim_{\mathbb{F}_p} B_S$$

where $S_\mathbb{C}$ *is the set of complex primes in* K.

The following lemma is crucial in proving Theorems 2–4 and in proving these theorems all we have to show that $B_{S_K} = 0$.

Lemma 16. *When* $p = 2$

(1) G_{S_K} *is free if and only if* K *is totally imaginary with a unique prime above* 2 *and* $B_{S_K} = 0$.
(2) $B_{S_K} = 0$ *if either the class number of* K *is odd or* S_K *generates the Sylow* 2*-subgroup of the class group of* K

Proof. (1) Since $p = 2$, $\{\pm 1\}$ belongs to K and $K_\wp$. Using (2) of Theorem 15 we see that G_{S_K} is free if and only if $\dim_{\mathbb{F}_2} B_{S_K} = 0$ and

$$\sum_{\wp \in S_K \setminus S_\mathbb{C}} \delta_\wp = \delta.$$

For the latter equality to hold, K should have a unique prime divisor of 2 and K should have no real embeddings. Hence we demand that there be a unique prime above 2 in K.

(2) Now, by (1) of Theorem 15 we see that $B_{S_K} = 0$ if and only if the group $Cl_{S_K}/Cl_{S_K}^2$ is trivial, where $Cl_{S_K} = Cl(K)/\langle S_K \rangle$. The group $Cl_{S_K}/Cl_{S_K}^2$ is trivial if and only if either h_K is odd or h_K is even and the Sylow 2-subgroup of Cl_{S_K} is trivial, which translates into saying that S_K generates the Sylow 2-subgroup of the class group of K. □

The following lemma is used in proving the main result.

Lemma 17. *Let* L *be a finite normal* p*-extension of a number field* K *in which at most divisors of* p *and infinity ramify. Let* S *be the divisors of* p *and infinity in* K *and similarly* $\tilde{S}$ *be the divisors*

of p and infinity in L; let G_S (respectively $G_{\tilde{S}}$) be the Galois groups of the maximal p-extensions of K (respectively L) unramified outside of S (respectively $\tilde{S}$). Then $G_{\tilde{S}}$ is a subgroup of G_S and has index $[L : K]$. In particular, if G_S is a free pro-p group, then $G_{\tilde{S}}$ is a free pro-p group.

2.2. Genus theory

We summarize well-known results in the following sections for the convenience of the reader.

Definition 18. [5, Chapter VI, p. 243] If K is any finite abelian extension of $\mathbb{Q}$, the genus field $\hat{K}$ of K is the largest abelian extension of $\mathbb{Q}$ contained in the Hilbert class field $\mathcal{K}$ of K. The extended genus field $\hat{K}^{(+)}$ of K is the largest abelian extension of $\mathbb{Q}$ contained in the extended Hilbert class field $\mathcal{K}^{(+)}$, where $\mathcal{K}^{(+)}$ is the maximal abelian extension of K unramified at the finite primes of K.

Theorem 19. [5, Chapter VI, Theorem 3.8] *Let $K = \mathbb{Q}(\sqrt{d})$ have discriminant Δ where $|\Delta| = p_1 p_2 \cdots p_t$ with $p_2, \ldots, p_t$ odd primes and p_1 is either an odd prime or a power of 2. Then the extended genus field is*

$$\hat{K}^{(+)} = \mathbb{Q}(\sqrt{d}, \beta_2, \ldots, \beta_t)$$

where

$$\beta_i = \begin{cases} \sqrt{p_i} & \text{if } p_i \equiv 1 \bmod 4, \\ \sqrt{-p_i} & \text{if } p_i \equiv 3 \bmod 4. \end{cases}$$

Consequently,

Theorem 20. [5, Chapter VI, Theorem 3.9] *If $K = \mathbb{Q}(\sqrt{d})$ is a quadratic extension of $\mathbb{Q}$ and if the discriminant Δ_K is divisible by exactly t different primes, then $[\hat{K}^{(+)} : K] = 2^{t-1}$.*

Note that $[\hat{K}^{(+)} : \hat{K}] \leqslant 2$. If K is complex or if K is real and some unit of the ring of algebraic integers of K has norm -1, then $\hat{K}^{(+)} = \hat{K}$ and the $\mathrm{Gal}(\hat{K}/K) \cong Cl(K)/Cl^2(K)$. Hence we have that $h_{\mathbb{Q}(\sqrt{d})}$ is even if $d < 0$ and discriminant of $\mathbb{Q}(\sqrt{d})$ has more than one prime factor. Therefore $\mathbb{Q}(\sqrt{-p})$ where p is a prime $\equiv 1 \bmod 4$ or $\mathbb{Q}(\sqrt{-2p})$, where p is an odd prime, have even class number. If $d > 0$ and discriminant of $\mathbb{Q}(\sqrt{d})$ has more than two prime factors then class number of $\mathbb{Q}(\sqrt{d})$ is necessarily even.

More precisely we have the result

Theorem 21. ([2, Corollary to Theorem 2.17] or [1, Corollary 18.4]) *The class number of a quadratic number field K is odd if and only if*

(1) $K = \mathbb{Q}(\sqrt{-1})$;
(2) $K = \mathbb{Q}(\sqrt{p})$, *p any prime*;
(3) $K = \mathbb{Q}(\sqrt{-p})$, *$p$ a prime* $\equiv 2, 3 \bmod 4$;
(4) $K = \mathbb{Q}(\sqrt{pq})$, *$p$ and q distinct primes,* $p \equiv 3 \bmod 4$ *and* $q = 2, 3 \bmod 4$.

Theorem 22. [2, Theorem 2.16] *Let $L/\mathbb{Q}$ be a cyclic extension of $\mathbb{Q}$ of degree l^n, l a prime. Let p_i, $1 \leqslant i \leqslant t$, be the finite set of primes, ramified in L, of ramification degrees l^{n_i}, $n_1 \geqslant n_2 \geqslant \cdots \geqslant n_t \geqslant 1$. Then* $\mathrm{Gal}(\hat{L}^{(+)}/L)$ *is abelian of type* $(l^{n_2}, \ldots, l^{n_t})$.

Theorem 23. [2, Theorem 2.17] *Let $L/\mathbb{Q}$ be an imaginary cyclic extension of degree 2^n $(n \geqslant 1)$. Then h_L is odd if and only if one finite rational prime ramifies in L.*

2.3. Class number parity

Proposition 24. [1, Corollary 19.6] *Let $K = \mathbb{Q}(\sqrt{d})$ be an imaginary quadratic extension of $\mathbb{Q}$. Then $h_K \equiv 2 \bmod 4$ if and only if*

(1) $d = -p, -2p$, *where p is prime congruent to* 5 mod 8;
(2) $d = -2q$ *where q is a prime congruent to* 3 mod 8;
(3) $d = -pq$ *with* $(\frac{q}{p}) = (\frac{p}{q}) = -1$ *where p is a prime* $\equiv 3 \bmod 4$ *and q is a prime* $\equiv 1 \bmod 4$.

Proposition 25. [1, Corollary 19.8] *For a real quadratic extension $K = \mathbb{Q}(\sqrt{d})$ with fundamental unit of norm -1, $h_K \equiv 2 \bmod 4$ if and only if*

(1) $d = 2q$, *with* $q \equiv 5 \bmod 8$;
(2) $d = q_1 q_2$ *with* $(\frac{q_2}{q_1}) = (\frac{q_1}{q_2}) = -1$

where q, q_1, q_2 are primes $\equiv 1 \bmod 4$.

Proposition 26. [1, Proposition 19.9] *Suppose $K = \mathbb{Q}(\sqrt{2q})$ or $\mathbb{Q}(\sqrt{q_1 q_2})$ with primes $q, q_1, q_2 \equiv 1 \bmod 4$ satisfying $q \equiv 5 \bmod 8$ or $(\frac{q_2}{q_1}) = (\frac{q_1}{q_2}) = -1$. Then the norm of the fundamental unit of K is -1.*

2.4. Dirichlet characters

A Dirichlet character is a multiplicative homomorphism $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$. The conductor of χ is the minimal n for which the map χ is defined. If χ is a character defined mod n, then χ is a character of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Let K be the fixed field of the kernel of χ. Then K is called the field belonging to χ and $\deg(K/\mathbb{Q}) =$ order of χ. If $n = \prod p^a$, then we may write any character χ defined mod n as $\chi = \prod \chi_p$, where χ_p is a character defined mod p^a. If X is a group of Dirichlet characters, then denote $X_p = \{\chi_p \mid \chi \in X\}$. A character is called even if $\chi(-1) = 1$ and odd if $\chi(-1) = -1$.

Theorem 27. [13, Theorem 3.5] *Let X be a group of Dirichlet characters and K the associated field. Let p be a prime number with ramification index e in K. Then $e = \#(X_p)$.*

3. Quadratic case

Proof of Theorem 2. Recall from Lemma 16 that if a number field has a real embedding then it cannot be 2-rational. Hence there are no real quadratic 2-rational number fields. For a quadratic number field with even class number, S_K will generate the Sylow 2-subgroup of the class group of K if and only if P_K is not principal and $h_K \equiv 2 \bmod 4$.

The genus number of an imaginary L as described in [3] is $\frac{e_1 \cdots e_n}{[L:\mathbb{Q}]}$, where $e_1, \ldots, e_n$ are the ramification indices of the ramifying primes $p_1, \ldots, p_n$ in L. If more than 2 finite primes ramify in $K = \mathbb{Q}(\sqrt{n})$, then by the Genus formula, $h_K \equiv 0 \bmod 4$. If $n = -1, -2$, or $-p$, where p is a prime congruent to 3 mod 8, then $h_{\mathbb{Q}(\sqrt{n})}$ is odd. If $n = -p$, where p is a prime congruent to 5 mod 8 or $n = -2p$, where p is a prime congruent to $3, 5 \bmod 8$ then $h_{\mathbb{Q}(\sqrt{n})} \equiv 2 \bmod 4$ by Proposition 24. Now we have to show that $P_{\mathbb{Q}(\sqrt{n})}$ is not principal. Hence, apply the norm to $K/\mathbb{Q}$. Hence $N_{K/\mathbb{Q}}(a + b\sqrt{-2p}) = a^2 + b^2(2p)$ which should equal $+2$. This cannot happen. Hence there are no algebraic integers of the form $a + b\sqrt{-2p}$ whose norm is 2, where $a, b \in \mathbb{Z}$. Whence $P_{\mathbb{Q}(\sqrt{n})}$ is not principal, and $P_{\mathbb{Q}(\sqrt{n})}$ generates the Sylow 2-subgroup of the class group of $\mathbb{Q}(\sqrt{n})$. Since $G_{S_{\mathbb{Q}(\sqrt{n})}}$ is a free pro-2 group on 2 generators by Theorem 15, $G_{S_{\mathbb{Q}(\sqrt{n})}} \cong \mathbb{Z}_2 \amalg \mathbb{Z}_2$.

If $n = -p$ where $p \equiv 1 \bmod 8$, or $n = -2p$ where $p \equiv 1, 7 \bmod 8$ then $h_{\mathbb{Q}(\sqrt{n})} \equiv 0 \bmod 4$ by Theorem 21 and Proposition 24. Now, suppose that the only ramifying primes in K are odd, say p and q. Then P_K is inert in K and $2 \mid h_K$. □

4. Cyclic case

Proof of Theorem 3. Observe that either $f_2 = 4$ or $e_2 \geqslant 2$. Note that every odd prime is tamely ramified in L. Suppose the conductor of L has a unique prime factor. Hence the conductor is either p or a power of 2. This is the case (1) and is easy to handle, because L is contained in $\mathbb{Q}(\zeta_p)$ or $\mathbb{Q}(\zeta_{2^4})$ respectively. But if L has conductor with two prime factors, then L is contained in $\mathbb{Q}(\zeta_{2^4 p})$ which is the case (2). Here, we need a more subtle analysis. Observe that at least one of the ramifying primes will have ramification index 4. By Genus theory (Section 2.2) we know that h_L is even. If $o(P_L) = 1$ or $8 \mid h_L$, then L cannot be 2-rational. If $o(P_L) = 2$ in $Cl(L)$, then by Lemma 16, L is 2-rational if and only if $2 \parallel h_L$ and similarly if $o(P_L) = 4$, then L is 2-rational if only if $2^2 \parallel h_L$. Note that if h_{L_+} is odd, then $o(P_L) \leqslant 2$.

If the conductor of L has more than two prime factors, i.e., if more than two finite primes ramify in L, using Genus theory (Theorem 22), it is easy to see that the Sylow 2-subgroup of the class group of L is too large for P_L to generate. We make use of Dirichlet characters to get information about L and L_+. Examples of fields L which satisfy the class number condition when the conductor has more than one prime factor, lie in $\mathbb{Q}(\zeta_{48})$ and $\mathbb{Q}(\zeta_{80})$. More details can be found in Section 9.

If $L/\mathbb{Q}$ is a totally imaginary degree 4 cyclic extension, then the unique degree 2 extension $L_+/\mathbb{Q}$ contained in L is totally real, because L_+ is the fixed field of complex conjugation. Observe that when a divisor of p ramifies in L/L_+, G_{S_L} is not a subgroup of $G_{S_{L_+}}$.

(1) Suppose L has conductor with a unique prime factor. Since $L/\mathbb{Q}$ is abelian, by the Kronecker–Weber theorem L is contained in a cyclotomic extension $\mathbb{Q}(\zeta_{p^r})$ for some prime p and $r \geqslant 1$. Then

$$\mathrm{Gal}\big(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}\big) \cong \big(\mathbb{Z}/p_1^{r_1}\big)^*.$$

Suppose $p \equiv 5 \bmod 8$. Then $4 \parallel p - 1$. Hence there exists a cyclic extension of degree 4 over $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_{p^r})$. The fixed field of the maximal subgroup of odd order in $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is a cyclic extension L of degree 4 over $\mathbb{Q}$. But 2 is inert in $L_+ = \mathbb{Q}(\sqrt{p})$, hence inert in L. Moreover, since $L/\mathbb{Q}$ is a totally imaginary cyclic extension of degree 4 and exactly one rational prime ramifies in $L/\mathbb{Q}$, h_L is odd by Genus theory (Theorem 23).

Table 1
Character table

	$o(\chi_1^a)$	$o(\chi_2^b)$	$o(\chi_3^c)$	L_+
1.	2	2	4	$\mathbb{Q}(\sqrt{p})$, $p \equiv 5 \bmod 8$
2.	1	2	4	–
3.	2	1	4	–
4.	1	1	4	–
5.	2	4	4	$\mathbb{Q}(\sqrt{2p})$, $p \equiv 1 \bmod 8$
6.	1	4	4	$\mathbb{Q}(\sqrt{2p})$, $p \equiv 5 \bmod 8$
7.	2	4	2	$\mathbb{Q}(\sqrt{2})$, $p \equiv 5 \bmod 8$
8.	1	4	2	$\mathbb{Q}(\sqrt{2})$, $p \equiv 3 \bmod 8$
9.	2	4	1	$\mathbb{Q}(\sqrt{2})$
10.	1	4	1	$\mathbb{Q}(\sqrt{2})$

If $p \equiv 3, 7 \bmod 8$, then 4 does not divide $p-1$ and hence there is no extension of degree 4 over $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_p)$. If $p \equiv 1 \bmod 8$, $\mathbb{Q}(\zeta_p)$ contains a cyclic extension L of degree 4 over $\mathbb{Q}$. But 2 factors in L where $\mathbb{Q}(\sqrt{p}) \subset L \subset \mathbb{Q}(\zeta_p)$.

If the conductor of L is a power of 2, then $L \subset \mathbb{Q}(\zeta_{2^4})$. Here L is the unique imaginary cyclic extension of $\mathbb{Q}(\zeta_{2^4})$ of degree 4. Note that $h_L = 1$.

(2) Now suppose L has conductor with two prime factors. Note that $L_+ = \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{p})$ or $\mathbb{Q}(\sqrt{2p})$. Therefore L is contained in $\mathbb{Q}(\zeta_{2^4 p})$. Then

$$\mathrm{Gal}\big(\mathbb{Q}(\zeta_{2^4 p})/\mathbb{Q}\big) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}.$$

Observe that the above decomposition of the $\mathrm{Gal}(\mathbb{Q}(\zeta_{2^4 p})/\mathbb{Q})$ is not unique. Also the character group of $\mathrm{Gal}(\mathbb{Q}(\zeta_{2^4 p})/\mathbb{Q})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}$. Now we introduce new notation for characters for the sake of convenience. Let χ_1 be a generator of $\mathbb{Z}/2\mathbb{Z}$, χ_2 be a generator of $\mathbb{Z}/4\mathbb{Z}$ and χ_3 be a generator of $\mathbb{Z}/(p-1)\mathbb{Z}$, chosen in such a way that $\mathbb{Q}(i)$ is the field of χ_1 and $\mathbb{Q}(\zeta_{2^4} + \zeta_{2^4}^{-1})$ is the field of χ_2. Hence χ_1 is an odd character and χ_2 is an even character. Every element of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}$ is of the form $\chi_1^a \chi_2^b \chi_3^c$, where $a \in \{0, 1\}$, $b \in \{0, 1, 2, 3\}$ and $c \in \{0, 1, \ldots, p-2\}$. Let $2^k \parallel p-1$. Then $\mathbb{Z}/(p-1)\mathbb{Z} \cong \mathbb{Z}/2^k\mathbb{Z} \times \mathbb{Z}/(\frac{p-1}{2^k})\mathbb{Z}$.

Since we are interested only in the degree 4, imaginary, cyclic extensions of $\mathbb{Q}$, we can assume without loss of generality that χ_3 is a generator of $\mathbb{Z}/2^k\mathbb{Z}$. Let the field of χ_3 be the fixed field of $\mathbb{Z}/(\frac{p-1}{2^k})\mathbb{Z}$, hence χ_3 is an odd character. We look for odd characters of order 4 with 2 and p as prime factors of the conductor i.e., characters with conductor $4p$, $8p$ or $16p$. Order of χ_1^a can be either 1 or 2, order of χ_2^b can be 1, 2, 4 and order of χ_3^c can be either $1, 2, \ldots, 2^k$ with the constraint that $o(\chi_1^a \chi_2^b \chi_3^c) = 4$. Moreover, since we demand that $\chi_1^a \chi_2^b \chi_3^c$ be an odd character, exactly one of χ_1^a or χ_3^c is odd. Table 1 gives all possible orders of χ_1^a, χ_2^b and χ_3^c to generate degree 4 cyclic extensions of $\mathbb{Q}$.

Let L_1, L_2 and L_3 denote the field of χ_1^a, χ_2^b and χ_3^c, L_{12} denote the field of $\chi_1^a \chi_2^b$ and let L denote the field of $\chi_1^a \chi_2^b \chi_3^c$. If $o(\chi_1^a) = 1$, then $L_1 = \mathbb{Q}$ and if $o(\chi_1^a) = 2$, then $L_1 = \mathbb{Q}(i)$. If $o(\chi_2^b) = 2$, then $L_2 = \mathbb{Q}(\sqrt{2})$ and if $o(\chi_2^b) = 4$, then $L_2 = \mathbb{Q}(\zeta_{2^4} + \zeta_{2^4}^{-1})$. Now, if $o(\chi_3^c) = 4$, then L_3 is a degree four cyclic extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_p)$ and if $o(\chi_3^c) = 2$, then $L_3 = \mathbb{Q}(\sqrt{\pm p})$, depending on whether $p \equiv \pm 1 \bmod 4$.

By Theorem 27, if $o(\chi_1^a \chi_2^b) = i$, then $e_2 = i$ in L and if $o(\chi_3^c) = j$, then $e_p = j$ in L, where $i, j \in \{1, 2, 4\}$. Moreover, if $e_2 = 4$ and $e_p = 4$, then $L_+ = \mathbb{Q}(\sqrt{2p})$, $4 \mid h_L$. If $e_2 = 4$ and

$e_p = 2$, then $L_+ = \mathbb{Q}(\sqrt{2})$, $2 \mid h_L$ and in both the cases $L \subset \mathbb{Q}(\zeta_{16p})$. Now, if $e_2 = 2$ and $e_p = 4$, then $L_+ = \mathbb{Q}(\sqrt{p})$ with $p \equiv 1 \bmod 4$, $2 \mid h_L$ and $L \subset \mathbb{Q}(\zeta_{8p})$. But if $e_2 = 4$ and $e_p = 1$, then $L \subset \mathbb{Q}(\zeta_{2^4})$, and if $e_2 = 1$ and $e_p = 4$, then $L \subset \mathbb{Q}(\zeta_p)$, hence we ignore lines 4, 9 and 10 from the character table. We also ignore lines 1 and 3, because the character $\chi_1^a \chi_2^b \chi_3^c$ is even. In line 5, χ_1^a is an odd character, moreover if $p \equiv 5 \bmod 8$ the character χ_3^c would also be odd. In lines 2 and 6, χ_1^a and χ_2^b are even, and the character χ_3^c would also be even if $p \equiv 1 \bmod 8$. From line 2 in the character table we see that $g_2 > 1$ in L if $p \equiv 1 \bmod 8$.

Now, let us have a closer look at line 5 of the character table. χ_1^a has order 2 and χ_2^b has order 4 and χ_3^c has order 4 hence they yield the following diagram of number fields.

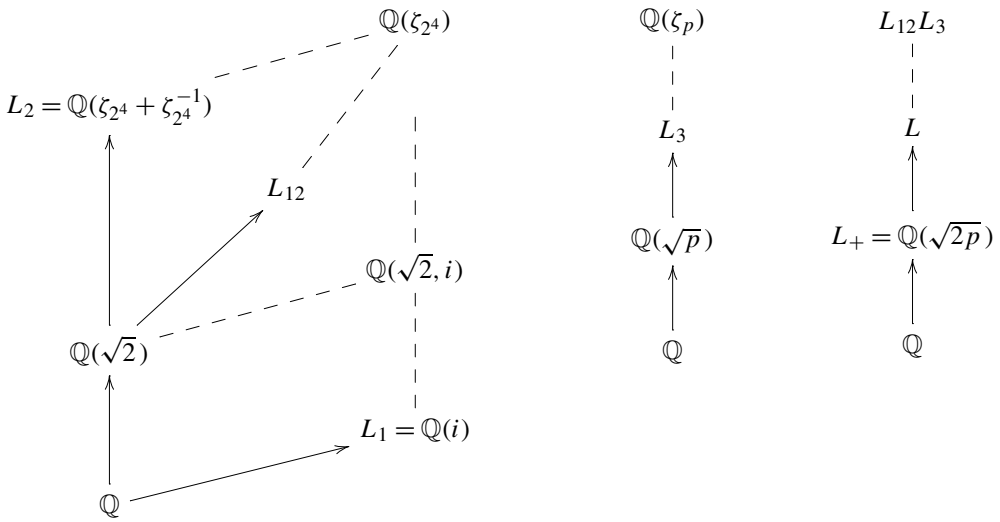

Diagram of number fields corresponding to line 5 of the character table.

Now χ_1^a is an odd character and χ_3^c is an even character. But, χ_3 being an odd character, implies that χ_3^c is an even power of χ_3. Hence the order of χ_3 is at least 8. Therefore, $p \equiv 1 \bmod 8$. Since $o(\chi_1^a \chi_2^b \chi_3^c) = 4$, $\deg(L/\mathbb{Q}) = 4$, also $\deg(L_{12}L_3/L) = 4$. Observe that $L_{12}L_3/L$ is an unramified extension as 2 is unramified in $\mathbb{Q}(\zeta_p)$ and p is unramified in $\mathbb{Q}(\zeta_{2^4})$. Observe that $4 \mid h_L$. If $4 \parallel h_L$, then $L_{12}L_3$ is the Hilbert 2-field of L. But $o(P_L) \leqslant 2$ as 2 splits in $\mathbb{Q}(\sqrt{p})$ and hence P_L factors in $L_{12}L_3$. Hence we ignore line 5. Looking at line 6 from the character table, we see that $f_2 = 4$ in L_3 and hence P_L is inert in $L_{12}L_3$. But, $B_{S_L} = 0$ if and only if $o(P_L) = 4$ and $4 \parallel h_L$.

Because of the requirement that $\chi_1^a \chi_2^b \chi_3^c$ be an odd character, in line 7 of the character table, odd primes, whose prime divisors ramify in L/L_+ are $\equiv 1 \bmod 4$ and similarly $\equiv 3 \bmod 4$ in line 8. Looking at line 7 of the character table it is easy to see that if $p \equiv 1 \bmod 8$, then 2 splits in $\mathbb{Q}(\sqrt{p})$, hence P_L factors in $L_{12}L_3$. But $o(P_L) \leqslant 2$. If $h_L \equiv 2 \bmod 4$, then $L_{12}L_3$ is the Hilbert 2-field of L and P_L splits in $L_{12}L_3$, whence P_L is principal.

In line 8 of the character table, observe that if $p \equiv 7 \bmod 8$, then 2 splits in $\mathbb{Q}(\sqrt{-p})$, and hence P_L splits in $L_{12}L_3$. Whence P_L is principal by an argument identical to the previous paragraph.

What is remaining to show that P_L is not principal in L. Now if p is a prime congruent to 5 mod 8 (3 mod 8 respectively), then $2^2 \parallel p - 1$ ($2 \parallel p - 1$ respectively). But 2 is inert in the

unique cyclic extension of $\mathbb{Q}$ of degree 4 (degree 2 respectively) contained in $\mathbb{Q}(\zeta_p)$. Note that 2 is unramified in $\mathbb{Q}(\zeta_p)$. Hence 2 can factor in $\mathbb{Q}(\zeta_p)$ into at most $\frac{p-1}{4}$ ($\frac{p-1}{2}$ respectively), both odd number of factors, and so 2 will factor into odd number of factors in $\mathbb{Q}(\zeta_{2^4 p})$. Hence P_L cannot be principal in L, for otherwise by the isomorphism of class group of L with $\mathrm{Gal}(\mathcal{L}/L)$, via the Artin map, where $\mathcal{L}$ is the Hilbert class field of L, P_L will factor in the genus field of L. Moreover if $L_+ = \mathbb{Q}(\sqrt{2p})$, then $f_2 = 4$ in L_3 and hence if $2^2 \parallel h_L$, then $o(P_L) = 4$.

Suppose the conductor of L has more than two prime factors, then Genus theory (Theorem 22) says that at least $4 \mid h_L$. Observe that for at least one of the ramifying primes, the ramification index will be 4. If $e_2 = 2$ in which case $o(P_L) \leqslant 2$ and $h_L \equiv 0 \bmod 4$. But if, $e_2 = 4$ then it is easy to see that either $o(P_L) \leqslant 2$ and $h_L \equiv 0 \bmod 4$ or $o(P_L) \leqslant 4$ and $h_L \equiv 0 \bmod 8$.

G_{S_L} is a free pro-2 group on 3 generators by (1) of Theorem 15. Therefore $G_{S_L} \cong \mathbb{Z}_2 \amalg \mathbb{Z}_2 \amalg \mathbb{Z}_2$. The description of the structure of $G_{S_{L_+}}$ will given in Section 6. □

5. Biquadratic case

Proof of Theorem 4. Since $g_2 = 1$, then either $e_2 = 2$ or $e_2 = 4$. Hence 2 is ramified in L. Observe that if $f_2 = 4$, then L is a cyclic extension of $\mathbb{Q}$. Suppose we know that at most 2 finite primes ramify in L. Then L is an imaginary Klein 4-subfield of $\mathbb{Q}(\zeta_{8p})$. The elementary 2-abelian quotient of $\mathrm{Gal}(\mathbb{Q}(\zeta_{8p})/\mathbb{Q})$ has rank 3. Hence there are 7 Klein 4-subfields, one of which is real. The remaining 6 are exactly those of Theorem 4, if $p \equiv \pm 3 \bmod 8$.

Unlike Theorem 3, Theorem 4 has no class number condition. The reason is because in Theorem 3 no subfield of L was 2-rational, while every L in Theorem 4 has a subfield which is 2-rational. Observe that since $F = \mathbb{Q}(\sqrt{k})$ where $k = \frac{mn}{(m,n)^2}$ is an imaginary subfield of L and L/F is unramified outside the prime above 2 and infinity, it suffices to show that F is 2-rational and by Lemma 17, L is 2-rational. But F in Theorem 4 is exactly one of the imaginary quadratic 2-rational number fields of Theorem 2. Also, observe that L_- is 2-rational by Theorem 2.

Lemma 28. *$B_{S_{L_+}} = 0$ if L_+ is any of the real quadratic subfields of $\mathbb{Q}(\zeta_{8p})$, where p is a prime $\equiv \pm 3 \bmod 8$.*

Proof. If $L_+ = \mathbb{Q}(\sqrt{p})$ where p is any prime, or if $L_+ = \mathbb{Q}(\sqrt{2p})$ where p is a prime $\equiv 3 \bmod 4$, then h_{L_+} is odd by Theorem 21.

If $m = 2p$ where $p \equiv 5 \bmod 8$, then $h_{L_+} \equiv 2 \bmod 4$ by Propositions 25 and 26. To show that P_{L_+} is not principal we apply norm to $L_+/\mathbb{Q}$. Suppose P_{L_+} is principal, then $N_{L_+/\mathbb{Q}}(a + b\sqrt{2p}) = a^2 - b^2(2p) = \pm 2$. Which implies that $a^2 \equiv \pm 2 \bmod p$. Since $-1 \equiv \square \bmod p$, we have $2 \equiv \square \bmod p$. But $2 \equiv \square \bmod p$ iff $p \equiv \pm 1 \bmod 8$. A contradiction. Hence there is no algebraic integer of norm ± 2 in L_+, and hence P_{L_+} is not principal in L_+. □

Now we determine the structure of $G_{S_{L_+}}$. Since L/L_+ is unramified outside P_{L_+} and the primes at infinity, G_{S_L} is a subgroup of index 2 in $G_{S_{L_+}}$. Moreover G_{S_L} has rank 3, hence we can apply Theorem 10. Observe that there are 3 primes above 2 and infinity in L_+, namely $\{P_{L_+}, \infty_1, \infty_2\}$. Therefore by the rank formula for $G_{S_{L_+}}$, we have 3 generators for $G_{S_{L_+}}$ and by the relations formula, $G_{S_{L_+}}$ has 2 relations. We have $G_{S_{L_+}}/Fr(G_{S_{L_+}}) \cong C_2 \times C_2 \times C_2$. Now by a trivial case of Leopoldt's conjecture, L_+ has a unique $\mathbb{Z}_2$-extension. Hence $G_{S_{L_+}}^{ab} \cong C_{2^k} \times C_{2^l} \times \mathbb{Z}_2$, for some $k, l \geqslant 1$. Hence, applying Theorem 10, we have that $G_{S_{L_+}} \cong (C_2 \times 1) \amalg (C_2 \times 1) \amalg \mathbb{Z}_2$ or $(C_2 \times \mathbb{Z}_2) \amalg (C_2 \times 1)$, but the latter has 3 relations and the former has only 2,

whence $G_{S_{L_+}} \cong C_2 \amalg C_2 \amalg \mathbb{Z}_2$ [see Remark 31 for further explanations on how we obtained the structure of $G_{S_{L_+}}$]. Thus $k = l = 1$. Hence by Lemma 17, we see that $G_{S_{L_+}}$ is a virtually free pro-2 group.

To complete the theorem we need the following auxiliary results.

Lemma 29. *If only two finite primes ramify in L, then L is 2-rational if and only if L is one of the imaginary biquadratic subfields of $\mathbb{Q}(\zeta_{8p})$ where $p \equiv \pm 3 \bmod 8$.*

Proof. We have already shown that if L is any one of the imaginary biquadratic subfields of $\mathbb{Q}(\zeta_{8p})$ where $p \equiv \pm 3 \bmod 8$, then L is 2-rational. To prove the converse, let L be any imaginary biquadratic subfield of $\mathbb{Q}(\zeta_{8p})$ where $p \equiv \pm 1 \bmod 8$. Then, $F = \mathbb{Q}(\sqrt{-2p})$ or $\mathbb{Q}(\sqrt{-p})$. Now, $h_F \equiv 0 \bmod 4$ or 2 splits in F. But L/F is totally ramified, whence $h_L \equiv 0 \bmod 4$ or 2 factors in L. But P_L^2 is principal. □

Proposition 30. *If more than two finite primes ramify in L, then L is not 2-rational.*

Proof. We are interested only in imaginary biquadratic fields L in which 2 ramifies and does not factor. If three finite primes 2, p and q ramify in L, then L is contained in $\mathbb{Q}(\zeta_{8pq})$, and L is one of the following biquadratic fields. $\mathbb{Q}(\sqrt{*p}, \sqrt{*q})$, $\mathbb{Q}(\sqrt{*2p}, \sqrt{*q})$, $\mathbb{Q}(\sqrt{*2p}, \sqrt{*2q})$, $\mathbb{Q}(i, \sqrt{*pq})$, $\mathbb{Q}(\sqrt{*2}, \sqrt{*pq})$ where $* = \pm$. If $e_2 = 4$ in L, then the genus number of L is 4 and the genus field $\hat{L}$ is a Klein 4-extension of L. Hence P_L cannot generate the 2-part of the class group of L.

However, if $e_2 = 2$ in L, then the genus number of L is 2 and the genus field $\hat{L}$ is a degree 2 extension of L. If $h_L \equiv 0 \bmod 4$, then P_L cannot generate the 2-part of the class group of L. But, if the $h_L \equiv 2 \bmod 4$, then we need more subtle analysis. Here we somehow need to show that P_L cannot generate the 2-part of the class group of L. One way to do this is by showing that P_L splits in $\hat{L}$. Observe that $\hat{L}$ is one of the following subfields of $\mathbb{Q}(\zeta_{8pq})$, namely $L(i)$, $L(\sqrt{*2})$, $L(\sqrt{*p})$ or $L(\sqrt{*q})$ where $* = \pm$. It is easy to see that $\hat{L}$ will contain $Q(\sqrt{d})$, where $d \equiv 1 \bmod 8$ and d is either $\pm p$, $\pm q$ or $\pm pq$. Observe that $\mathbb{Q}(\sqrt{d})$ does not lie in L. But 2 splits in $\mathbb{Q}(\sqrt{d})$, where $d \equiv 1 \bmod 8$, and hence P_L will split in $\hat{L}$. Then we can show that P_L is principal in L by looking at the Artin map restricted to the Sylow 2-subgroup of the ideal class group of L.

Suppose more than 3 finite primes ramify in L. If $e_2 = 2$ then P_L^2 is principal. Using the genus formula, the genus number of L is multiple of 4 and hence $h_L \equiv 0 \bmod 4$. Similarly, if $e_2 = 4$, then the genus number of L is multiple of 8 and the $h_L \equiv 0 \bmod 8$. □

Remark 31. In the argument given in the proof of Theorem 4 for capturing the structure of $G_{S_{L_+}}$, we do not consider the case when $G_{S_{L_+}} \cong (C_2 \times \mathbb{Z}_2) \amalg \mathbb{Z}_2$, even though it has 2 relations and 3 generators which is exactly what we are after. The reason is the following. Suppose G is a pro-p group and $G = H \amalg F$, where H and F are pro-p groups. Then the abelianisation of G; namely $G^{ab} = H^{ab} \times F^{ab}$. Note that the free pro-p product becomes a direct product in the abelianisation. Hence if we were to go with the above structure of $G_{S_{L_+}}$, then $G_{S_{L_+}}^{ab}$ would be $C_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Which would imply that L_+ has 2 independent $\mathbb{Z}_2$-extensions. A contradiction.

Remark 32. It is known that the p-rational fields satisfy Leopoldt's conjecture [8]. A natural question is whether the virtually free pro-p fields, i.e., number fields K, for which the G_S is

virtually free, satisfy Leopoldt's conjecture. The answer is yes. Because, virtually free pro-p fields have a field extension which is p-rational, and by [9, Proposition 10.3.13] if the Leopoldt's conjecture is true for a prime p and a number field K, then it is also true for p and every subfield of K.

Remark 33. If m is a prime congruent to 3 mod 8 and $n = -1$ or if $m = 2p$ where p is a prime congruent to 3 mod 8 and $n = -2$, then G_{S_L} is the inertia subgroup of $G_{S_{L_+}}$ for the prime P_{L_+}. Note that in case (c), G_{S_L} is not a subgroup of $G_{S_{L_+}}$.

Remark 34. The cohomological dimension of G_{S_L} is one, since G_{S_L} is a free pro-2 group [12, p. 23]. But the cohomological dimension of $G_{S_{L_+}}$ is infinity, since $G_{S_{L_+}} \cong C_2 \amalg C_2 \amalg \mathbb{Z}_2$ and using [9, Theorem 4.1.4] and observing that C_2 is cyclic.

6. Cyclic case revisited

We will describe the structure of $G_{S_{L_+}}$ of Theorem 3. Observe that except in the case when 2 is the only ramifying prime in L, G_{S_L} is not a subgroup of $G_{S_{L_+}}$ as divisors of odd primes ramify in L/L_+. Hence we cannot apply Theorem 10 directly. Observe that every L_+ of Theorem 3 is one of the L_+ of Theorem 4, hence we see that the biquadratic number field L of Theorem 4 is a degree 2 extension of L_+ which is unramified outside the primes above 2 and infinity. Hence the structure of $G_{S_{L_+}}$ of Theorem 3 is identical to the structure of $G_{S_{L_+}}$ of Theorem 4.

7. Virtually free case

Proof of Corollary 5. All the degree 4 extensions of $\mathbb{Q}$ we investigate in this paper are normal. Theorem 4 characterizes all degree 4 normal extensions of $\mathbb{Q}$ which are 2-rational and contain K, hence the proof follows. Observe that K is virtually free. □

8. Minimal 2-rational case

Proof of Corollary 7. Observe that $G_{S_{\mathbb{Q}}} \cong C_2 \amalg \mathbb{Z}_2$ by Theorem 15, hence $\mathbb{Q}$ is not minimal 2-rational. By Theorem 4, it is easy to see that no biquadratic extension of $\mathbb{Q}$ is minimal 2-rational. Hence any minimal 2-rational degree 4 normal extension of $\mathbb{Q}$ must be cyclic over $\mathbb{Q}$. Proof of the cyclic case follows from Theorem 3. □

9. Examples of L for conductor with prime power factors in Theorem 3

Here is a compiler ready Magma code to show that number field L exists with the given class number condition.

```
K := CyclotomicField(80);
M := SubfieldLattice(K);
for ent in M do
  L := NumberField(ent);
  if Degree(L) eq 4 then
    N := SubfieldLattice(L);
    for ent in N do
```

```
        F := NumberField(ent);
        if Degree(F) eq 2 then
           print "sig =", Signature(L), "clnum =", #ClassGroup(L),
           "sig =", Signature(F), "clnum =", #ClassGroup(F);
        end if;
      end for;
    end if;
end for;
```

The program loops through all the degree 4 extensions L of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_{80})$ and then for each L it loops through all the quadratic extensions F of $\mathbb{Q}$ contained in L. The signature(L) gives the number of real embeddings followed by the number of pairs of complex embeddings of L and the "*clnum*" gives the order of the class group. If L is totally imaginary cyclic of degree 4, then it will have only one quadratic subfield F, moreover F being real. Observe that if $F = \mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{5})$, then $h_F = 1$ and by Genus theory h_L is even if the conductor of L has more than one prime factor. If $F = \mathbb{Q}(\sqrt{10})$, then $h_F = 2$ and by Genus theory $4 \mid h_L$.

Now, $\chi_3 : (\mathbb{Z}/5\mathbb{Z})^\times \to \mathbb{C}^\times$, defined by $\chi_3(2) = i$. Now if $c = 1$, then $o(\chi_3) = 4$ and the field of $\chi_3 = L_3 = \mathbb{Q}(\zeta_5)$. Moreover, χ_1 is a generator of $\mathbb{Z}/2\mathbb{Z}$. Now, looking at lines 2 and 6 of the character table, one observes that $a = 2$ and hence $o(\chi_1^2) = 1$. If $b = 1$, then $o(\chi_2) = 4$. Therefore $L_+ = \mathbb{Q}(\sqrt{10})$. Looking at the output of the Magma code one can see that $h_L = 4$ or 20. Observe that there are two fields above $L_+ = \mathbb{Q}(\sqrt{10})$. One of them is generated by $\chi_1^2\chi_2\chi_3$ and the other by $\chi_1^2\chi_2\overline{\chi_3} = \chi_1^2\chi_2\chi_3^3$. But in either case $2^2 \parallel h_L$. Now, if $b = 2$, then $o(\chi_2^2) = 2$ and using the character table one can see that $L_+ = \mathbb{Q}(\sqrt{5})$ and $h_L = 2$. Let us consider the case when $c = 2$. Then $o(\chi_3^2) = 2$ and the field of $\chi_3^2 = L_3 = \mathbb{Q}(\sqrt{5})$. Again using the table one can observe that $b = 1$ and $a = 1$ and $L_+ = \mathbb{Q}(\sqrt{2})$. The output of the Magma code gives $h_L = 2$.

The Magma code when L is contained in $\mathbb{Q}(\zeta_{48})$ is identical. Here $\chi_3 : (\mathbb{Z}/3\mathbb{Z})^\times \to \mathbb{C}^\times$, defined by $\chi_3(2) = -1$ and the field of $\chi_3 = L_3 = \mathbb{Q}(\sqrt{-3})$. Line 8 of the table says that $c = 1$, $b = 1$ and $a = 2$. Hence $L_+ = \mathbb{Q}(\sqrt{2})$. Then one can see from the Magma output that $h_L = 2$.

10. Future work

To characterize quadratic number fields which are not 2-rational but have a degree 2^n, $n \geqslant 1$, extension not necessarily Galois over $\mathbb{Q}$, but are 2-rational. Also, characterize p-rational number fields and virtually free number fields K which have a degree p-extension L such that L is p-rational and L/K is unramified outside the prime divisors of p and infinity, where p is odd.

Acknowledgments

I express my deep gratitude to my co-adviser Prof. Stephen V. Ullom for his invaluable time and numerous helpful conversations and my adviser Prof. Nigel Boston for suggesting the problem. I also thank Mark Norfleet for helping me with TeXing.

References

[1] P.E. Conner, J. Hurrelbrink, Class Number Parity, World Scientific, 1988.
[2] A. Fröhlich, Central Extensions, Galois Groups, and Ideal Class Groups of Number Fields, Contemp. Math., vol. 24, Amer. Math. Soc., 1983.

[3] Y. Furuta, The genus field and genus number in algebraic number fields, Nagoya Math. J. 29 (1967) 281–285.
[4] W.N. Herfort, L. Ribes, P.A. Zalesskii, p-Extensions of free pro-p groups, Forum Math. 11 (1999) 49–61.
[5] G.J. Janusz, Algebraic Number Fields, Amer. Math. Soc., 1996.
[6] H. Koch, Galoissche Theorie der p-Erweiterungen, Deutscher Verlag der Wissenschaften, Berlin, 1970.
[7] H. Koch, Galois Theory of p-Extensions, Springer, 2002.
[8] H. Miki, On the maximal abelian l-extension of a finite algebraic number field with given ramification, Nagoya Math. J. 70 (1978) 183–202.
[9] J. Neukirch, A. Schmidt, K. Wingberg, Cohomology of Number Fields, Springer, 1999.
[10] L. Ribes, P. Zalesskii, Profinite Groups, Springer, 2000.
[11] J.P. Serre, Trees, Springer, 1980.
[12] J.P. Serre, Galois Cohomology, Springer, 2002.
[13] L.C. Washington, Introduction to Cyclotomic Fields, Springer, 1982.
[14] K. Wingberg, On Demuškin groups with involution, Ann. Sci. Ecole Norm. Sup. (4) 22 (4) (1989) 555–567.
[15] P.A. Zalesskii, On virtually projective groups, J. Reine Angew. Math. 572 (2004) 97–110.